OIPE JC68 AUG 11 2004 PATENT & TRADEMARK OFFICE

PATENT APPLICATION
Do. No. 5038-12

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Sultan Weatherspoon and Duncan Glendinning

Serial No.	09/389,437	Examiner:	Lee, Chi Chung
Confirm. No.	5396	Group Art Unit:	2131
Filed:	September 3, 1999		

For: SECURE WIRELESS LOCAL AREA NETWORK

RECEIVED
AUG 1 2 2004
Technology Center 2100

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

The enclosed Appeal Brief is in furtherance of the Notice of Appeal mailed in this case on June 9, 2004. Appeal is taken from the Examiner's Office Action mailed May 21, 2004, finally rejecting claims 1-20.

Also enclosed:

☒ Form PTO-2038 authorizing payment in the amount of $440.00 for an Appeal fee of ($330.00) and a 1-month Extension fee of ($110.00).

☒ Any deficiency or overpayment should be charged or credited to deposit account no. 13-1703.

Customer No. 20575

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

08/11/2004 SZEWDIE1 00000064 09389437
02 FC:1251 110.00 OP

Graciela G. Iowger
Reg. No. 42,444

MARGER JOHNSON & McCOLLOM, P.C.
1030 SW Morrison Street
Portland, OR 97205
(503) 222-3613

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
Date: August 9, 2004

Lisbeth A. Nichols

AUG 11 2004
PATENT & TRADEMARK OFFICE

PATENT APPLICATION
Attorney Do. No. 5038-12

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Sultan Weatherspoon and Duncan Glendinning

Serial No.	09/389,437	Examiner:	Lee, Chi Chung
Confirm. No.	5396	Group Art Unit:	2131
Filed:	September 3, 1999		
For:	SECURE WIRELESS LOCAL AREA NETWORK		

RECEIVED
AUG 1 2 2004
Technology Center 2100

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF
UNDER 37 CFR §1.192

Appeal is taken from the Examiner's Office Action mailed May 21, 2004, finally rejecting claims 1-20 in the instant application.

This Appeal Brief is in furtherance of the Notice of Appeal mailed in this case on June 9, 2004.

The fees required under §1.17(c) and any required petition for extension of time for filing this Brief and fees therefor are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This Brief is transmitted in triplicate.

08/11/2004 SZEWDIE1 00000064 09389437
01 FC:1402 330.00 OP

This Brief contains these items under the following headings, and in the order set forth below.

TABLE OF CONTENTS

RECEIVED

AUG 1 2 2004

Technology Center 2100

I. REAL PARTY IN INTEREST
37 CFR §1.192(c) (1)

The present application has been assigned to:

INTEL CORPORATION

2200 Mission College Blvd.

P.O. Box 58119

Santa Clara, CA 95052-8119

II. RELATED APPEALS AND INTERFERENCES
37 CFR §1.192(c) (2)

The Board's decision in the present Appeal will not directly affect, or be directly affected, or have any bearing on any other appeals or interferences known to the appellant, or to the appellant's legal representative.

III. STATUS OF CLAIMS
37 CFR §1.192(c) (3)

Status of all the Claims:

1. Claims presented: 1-20.
2. Claims withdrawn from consideration but not cancelled: None.
3. Claims canceled: None.
4. Claims pending: 1-20, of which:
    a. claims allowed: None.
    b. claims rejected: 1-20.

The appellant appeals the rejection of claims 1-20, having been finally twice rejected by the Examiner.

IV. STATUS OF AMENDMENTS

37 CFR §1.192(c) (4)

Subsequent to the last Office Action mailed February 9, 2004, an amendment was filed by applicant on May 10, 2004, and was entered.

V. SUMMARY OF THE INVENTION
37 CFR §1.192(c) (5)

The secure LAN of the present invention includes a wireless device for use by a wireless device operator. An access point is connected to a wired LAN in communication with the wireless device through an air channel for authenticating the wireless device. An authentication server is connected to the wired LAN for providing the operator with access to the wired LAN after authenticating the access point, the wireless device, and the operator. Summary of the Invention, page 4, lines 5-9.

The network operates as shown in FIGS. 3A-C. At step 300, the first and second authentication devices 104A and 108A, respectively, are installed in the AP 102A and in the wireless device 106A, respectively. An operator establishes an air communications channel 114 between the wireless device 106A and the AP 102A (step 302). During the establishment of the air channel 114, the AP 102A and the wireless device 106A exchange the encryption mechanism to be used in future communications. At step 304, the first authentication device 104A generates a first authentication message that includes validating information about the AP, e.g., an AP key unique to the AP 102A. The AP key may be a digital signature. A digital signature is a block of data at the end of a message that attests to the authenticity of the file and, consequently, of the AP 102A. If any change is made to the file, the signature will not verify. Thus, digital signatures perform both an authentication and message integrity function. The AP encrypts (step 306) and transmits (step 308) the first authentication message to the wireless device 106A. The wireless device 106A receives and decrypts (step 310) the first authentication message and determines whether the AP is a valid access point to the wired LAN 120 (step 312). Authenticating the AP by analyzing the first authentication message ensures that the AP is authorized to be connected to the wired LAN 120 and that it is not a rogue AP set up to facilitate or gain unauthorized access to the wired LAN 120.

If the AP 102A is not valid, the air communications channel is disabled and communications between the AP 102A and the wireless device 106A terminate (step 314). If the AP 102A is valid, the second authentication device 108A generates (step 316) a second authentication message that, at a minimum, includes a device key identifying the second authentication device 108A as well as the operator's logon name and password. The device key may be known or unknown to the operator. Validation of the wireless device 106A may involve a challenge response in which the AP 102A requests a certain type of validation from the wireless device 106A, e.g., a digitally signed message. The

second authentication device 108A encrypts (step 318) and transmits (step 320) the second authentication message to the AP 102A over the air channel 114. The AP 102A receives the second authentication message and decrypts the portion of the message that includes the device key. At step 322, the AP 102A analyzes the decrypted portion of the second authentication message, i.e., the device key, to determine whether the wireless device 106A is valid.

If the device key is invalid (step 324), the air communications channel is disabled and communications between the AP 102A and the wireless device 106A terminate (step 314).

If the device key verifies (step 324), that is, if the wireless device 106A is valid, the AP 102A establishes a control channel 112 with the authentication server 110 at step 326. The AP 102A then transmits (step 328) the encrypted first authentication message and the encrypted portion of the second authentication message that includes the operator's logon name and password to the authentication server 110.

The authentication server 110 decrypts the first authentication message to verify that the AP 102A is valid (step 330). The authentication server then decrypts the second authentication message to verify the operator's logon name and password (step 330). The authentication server 110 verifies the operator's logon name and password by, e.g., comparing the received logon name and password to a stored list of authorized user names and passwords. If both or either of the AP 102A and the operator are invalid (step 332), the authentication server 110 will deny access to the wired LAN 120 (step 334). If the authentication server 110 validates both the AP and the operator (step 332), the authentication server 110 will enable access to the wired LAN 120 at step 336. The authentication server 110 will enable access to the wired LAN 120 by, e.g., establishing a data channel between the AP and any other device on the wired LAN 120. That is, the authenticated AP and operator will have access to all LAN 120 resources available to wired devices such as devices 16A-D.

Specification, page 5, line 27 – page 7, line13.

VI. ISSUES ON APPEAL
37 CFR §1.192(c) (6)

Whether claims 1 and 9 are anticipated under 35 U.S.C. 102(e) by Holmes (U.S. Pat No. 6,334,056).

Whether claims 2-8, 10-12 and 14-20 are unpatentable under 35 U.S.C. § 103(a) over Holmes in view of Nevoux et al (U.S. 5,661,806A).

Whether claim 13 is unpatentable under 35 U.S.C. § 103(a) over Holmes in view of Nevoux et al and in further view of Data Dictionary.

VII. GROUPING OF CLAIMS
37 CFR §1.192(c) (7)

The following grouping of claims identifies claims that stand or fall together.

Group A: Claims 1 and 9.

Group B: Claims 2 and 10.

Group C: Claims 3 and 11.

Group D: Claims 4 and 12.

Group E: Claims 5 and 13.

Group F: Claims 6, 7 and 14.

Group G: Claims 8, 15, and 20.

Group H: Claims 16 and 19.

Group I: Claims 17 and 18.

VIII. ARGUMENT
37 CFR §1.192(c) (8)

The Prior Art

In the final rejection, the Examiner applied two U.S. Patents: 6,334,056, issued to Holmes et al. ("Holmes"), and 5,661,806A, issued to Nevoux et al. ("Nevoux"). A short description of the Homes and Nevoux references follows.

The Holmes Reference

Holmes' invention allow sa handheld device secure access to a limited access data network or intranet. (Holmes, abstract). To achieve this end, the handheld device transmits a radio signal, that when received at a cell tower, is transformed into electrical signals that are ultimately sent to a data network. (Holmes, figure 1; col. 3, ll. 3-20.) In one embodiment shown, the data network is the World Wide Web or Internet. (Holmes, col. 3, ll. 16-34.) Once the electrical signals are in the data network they can be routed to the intranet, via an intranet interface, where the intranet interface authenticates the handheld device and operator. (Holmes, col. 4, ll. 4-6 and 21-37).

Holmes' Figure 3 shows an embodiment of the interface between the data network and the intranet. The interface comprises a router 30, with an incorporated firewall 32, and a proxy server 34. Router 30 receives data from data network and transfers it to either proxy server 34 or to Other Internet Application. When the data is transferred to proxy server 34, it is always sent through firewall 32 to be inspected. Holmes, col. 4, ll. 14-15. This inspection involves determining whether firewall 32 recognizes the wireless service provider for the handheld device. Holmes, col. 5, ll. 3-13 and 27-36. If it does not recognize then the firewall rejects the data. If firewall 32 recognizes then the data is sent to proxy server 34 to authenticate the wireless device and operator.

The Nevòux Reference

Nevoux's invention controls access to a telecommunications network by requiring authentication of a terminal and its corresponding user module. (Holmes, summary of the invention). Authentication of the terminal and the user module occur in the access system SAA upon receipt of session keys corresponding to the terminal and the user module. Nevoux, col. 4, ll. 40 – col. 5, ll. 25. Nevoux's system creates two sets of session keys, one in the home location register HLR and visitor location register VLR, and the other in the terminal PA and user module SIM. Nevoux, col. 4, ll. 40 – col. 5, ll. 25. These sets of

keys are then compared in the VLR to authenticate both the PA and the SIM. Nevoux, col. 4, ll. 40 – col. 5, ll. 25. Once authenticated SAA allows PA access to the network STN.

The Holmes Reference Does Not Anticipate the Claims of Group A

Group A contains claims 1 (independent) and 9 (independent). The following analysis uses claim 1 as a representative claim for this Group, as that is the independent claim that the Examiner addressed explicitly.

Claim 1 recites *an access point coupled to the wired computer LAN in communication with the wireless device through an air channel to authenticate the wireless device without going through the firewall.* According to the Examiner's final rejection, Holmes's router 30 and application(s) 38 disclose the recited access point and wired computer LAN, respectively. Final Office Action at pages 2-3. Router 30, however, is not *coupled* to application(s) 38, and therefore cannot disclose the recited *access point.*

The Examiner's final rejection further states that Holmes's wireless device 10 and firewall 32 disclose the recited wireless device and firewall, respectively. Final Office Action at pages 2-3. Holmes, however, does not enable router 30 to authenticate wireless device 10, rather it only verifies that the URL received through the Internet is of a known wireless service provider. Holmes, col. 5, ll. 3-13 and 27-36. Holmes, further, discloses a system in which "all traffic to and from the intranet passes through this firewall" 32, therefore all traffic to the intranet from wireless device 10 must pass through firewall 32. Holmes, col. 4, ll. 14-15. Since router 30 cannot authenticate wireless device 10, nor do so without going through firewall 32, router 30 cannot disclose the recited *access point.* Holmes, therefore, does not anticipate claims 1 and 9.

Claim 1 further recites *an authentication server ... to provide the operator with access to the wired LAN after authenticating the access point, the wireless device, and the operator without going through the firewall.*

According to the Examiner's final rejection, Holmes's proxy server 34 discloses the recited authentication server. Final Office Action at pages 2-3. Holmes, however, does not enable proxy server 34 to *authenticate an access point.* Holmes, col. 5, ll. 14-67; Figure 4. Proxy server 34, further, only receives traffic from firewall 32 and therefore cannot authenticate any device *without going through a firewall.* Holmes, col. 5, ll. 3-13; col. 4, ll. 14-15. Since proxy server 34 cannot authenticate an access point, nor do so without going through firewall 32, proxy server 34 cannot disclose the recited

authentication server. Holmes, therefore, does not anticipate claims 1 and 9.

In summary, Examiner's reference does not teach or suggest the limitations of claims 1 and 9, under any reasonable interpretation of those limitations. Thus the claims of Group A are not anticipated and must be allowed. Applicant respectfully requests that the Examiner's final rejection of the claims of Group A be overturned.

The Nevoux and Holmes References Cannot Support a Proper *Prima Facie* Case of Obviousness for the Claims of Group B

An obviousness rejection must demonstrate that the claimed invention as a whole would be obvious in light of the applied references. *See, e.g., Stratoflex, Inc. v. Aeroquip Corp.*, 218 USPQ 871 (Fed. Cir. 1983). A *prima facie* case of obviousness requires, among other things, that the applied references teach or suggest *every limitation* found in a rejected claim. *See In re Wilson*, 165 USPQ 494, 496 (CCPA 1970) ("all words in a claim must be considered in judging the patentability of that claim against the prior art"); *see generally* Manual of Patent Examining Procedure § 2143.03. An obviousness rejection is deficient on its face when the prior art fails to at least suggest all the elements of the invention. Such is the case with respect to the claims at issue here.

Group B contains claims 2 (dependent from 1) and 10 (dependent from 9). Accordingly, those claims are patentable for the same reasons presented above for the claims of Group A. But these claims also contain further limitations not suggested by the prior art. The following analysis uses claim 10 as a representative claim for this Group, as that is the dependent claim that the Examiner addressed explicitly.

Claim 10 recites *the access means includes a first authentication means to generate, encrypt, and transmit a first authentication message to the wireless means, the first authentication message including validating information about the access means.* According to the Examiner's final rejection, Nevoux's SAA, VLR, and PA disclose the recited access means, first authentication means, and wireless means, respectively. Final Office Action at pages 4-5. The Examiner's rejection further states that random numbers R1 and R2 disclose the recited first authentication message. Final Office Action at pages 4-5. Random numbers R1 and R2, however, are used by PA and SIM (user module associated with PA) to generate session keys, which are subsequently sent to VLR and used to authenticate PA and SIM. Nevoux, col. 4, ll. 50-52 and 56-65. Since, random numbers R1 and R2 do not include information about validating SAA, VLR cannot disclose the recited *first authentication means.* Furthermore, Nevoux's system does not

enable the authentication of SAA and thus VLR cannot generate or transmit a *first authentication message.*

Nevoux, further, does not disclose or enable the ability to encrypt random numbers R1 and R2, prior to their transmission to PA. Nevoux, col. 4, ll. 8-11, 24-28 and 40-55. Since, Nevoux does not disclose the ability of VLR to encrypt random numbers R1 and R2, VLR cannot disclose the recited *first authentication means.*

In summary, neither of the Examiner's references teach or suggest the limitations of claims 2 and 10, under any reasonable interpretation of those limitations. Thus combining the references, as the Examiner suggests, is to no avail. A *prima facie* case of obviousness is lacking, and the claims of Group B must be allowed. Applicant respectfully requests that the Examiner's final rejection of the claims of Group B be overturned.

The Nevoux and Holmes References Cannot Support a Proper *Prima Facie* Case of Obviousness for the Claims of Group C

Group C contains claims 3 (dependent from 2) and 11 (dependent from 10). Accordingly, those claims are patentable for the same reasons presented above for the claims of Group A. But these claims also contain further limitations not suggested by the prior art. The following analysis uses claim 11 as a representative claim for this Group, as that is the dependent claim that the Examiner addressed explicitly.

Claim 11 recites *the wireless device includes a second authentication means to generate, encrypt, and transmit a second authentication message to the access means, the second authentication message including validating information about the wireless device and the operator.* According to the Examiner's final rejection, Nevoux's SIM discloses the recited second authentication means. Final Office Action at pages 4-5. The Examiner's rejection further states that identification parameters IMUI and IMTI disclose the recited second authentication message. Final Office Action at pages 4-5. Identification parameter IMTI is generated by PA, and identification parameters IMUI and IMTI are transmitted to SAA by PA. Since, identification parameter IMTI is not generated by SIM nor is identification parameters IMUI and IMTI are transmitted to SAA by SIM, SIM cannot disclose the recited *second authentication means.*

Nevoux, further, does not disclose or enable the ability to encrypt identification parameters IMUI and IMTI, prior to their transmission to SAA. Nevoux, col. 4, ll. 8-11,

24-28 and 40-55. Since, Nevoux does not disclose the ability of SAA to encrypt identification parameters IMUI and IMTI, SIM cannot disclose the recited *second authentication means.*

In summary, neither of the Examiner's references teach or suggest the limitations of claims 3 and 11, under any reasonable interpretation of those limitations. Thus combining the references, as the Examiner suggests, is to no avail. A *prima facie* case of obviousness is lacking, and the claims of Group C must be allowed. Applicant respectfully requests that the Examiner's final rejection of the claims of Group C be overturned.

The Nevoux and Holmes References Cannot Support a Proper *Prima Facie* Case of Obviousness for the Claims of Group D

Group D contains claims 4 (dependent from 3) and 12 (dependent from 11). Accordingly, those claims are patentable for the same reasons presented above for the claims of Group A. But these claims also contain further limitations not suggested by the prior art. The following analysis uses claim 12 as a representative claim for this Group, as that is the dependent claim that the Examiner addressed explicitly.

Claim 12 recites *the first authentication means transmits the first and second authentication messages to the authentication means after authenticating the wireless device.*

According to the Examiner's final rejection, Nevoux's HLR discloses the recited authentication means. HLR, however, does not receive the random numbers R1 and R2 and the identification parameters IMUI and IMTI after VLR authenticates the PA. Nevoux, col. 5, ll. 18-25. For Nevoux's system to function properly both the random numbers and the identification parameters must be sent to the HLR prior to authentication, where they are used to generate SRES keys necessary for VLR to authenticate the wireless means. Nevoux, col. 4, ll. 52-55. Since, Nevoux does not disclose the ability of the authentication means to receive random numbers R1 and R2 and identification parameters IMUI and IMTI after VLR authenticates the PA, HLR cannot disclose the recited *authentication means.*

Furthermore, with reference to independent claim 9 that claim 12 depends, Nevoux's HLR does not disclose any of the recited authentication means. The Examiner alleges that Nevoux's STN discloses the recited wired computer LAN. Office Action,

dated 7/29/2003, page 3. HLR, however, is not *coupled* to STN, nor does HLR enable the *operator's access through a wireless means* to the wired computer LAN. Nevoux, Figure 1; col. 4, ll. 40 - col. 5, ll. 25. HLR, further, does not *authenticate* any device or means. Nevoux, col. 4, ll. 40 - col. 5, ll. 25. Since HLR does not meet any of the limitations of claim 9 upon which claim 12 depends, HLR cannot disclose the recited *authentication means*.

In summary, neither of the Examiner's references teach or suggest the limitations of claims 4 and 12, under any reasonable interpretation of those limitations. Thus combining the references, as the Examiner suggests, is to no avail. A *prima facie* case of obviousness is lacking, and the claims of Group D must be allowed. Applicant respectfully requests that the Examiner's final rejection of the claims of Group D be overturned.

The Nevoux, Holmes, and Data Dictionary References Cannot Support a Proper *Prima Facie* Case of Obviousness for the Claims of Group E

Group E contains claims 5 (dependent from 3) and 13 (dependent from 11). Accordingly, those claims are patentable for the same reasons presented above for the claims of Group A. But these claims also contain further limitations not suggested by the prior art. The following analysis uses claim 13 as a representative claim for this Group, as that is the dependent claim that the Examiner addressed explicitly.

Claim 13 recites *the first and second authentication means are smart cards*. The Examiner's final rejection stated, in part, that:

> "[a]s disclosed in computer dictionary, use of smart card was known prior to applicant's filing date. Motivation to include the components of the VLR (i.e. the first authentication means) in the smart card is to allow the access system to update the terminal location information in the database 12 [see Nevoux column 5 lines 62-67]." Final Office Action, page 6.

The assertions in this statement, as to the motivation to combine the references, are not persuasive since the recited smart cards are primarily used to "identify a specific user," from a plurality of different users. Specification, page, 5, lines 11-18. Nevoux's system only comprises one VLR and thus there is no motivation to incorporate the VLR into the recited smart card.

In summary, none of the Examiner's references teach or suggest the limitations of

claims 5 and 13, under any reasonable interpretation of those limitations. Thus combining the references, as the Examiner suggests, is to no avail. A *prima facie* case of obviousness is lacking, and the claims of Group E must be allowed. Applicant respectfully requests that the Examiner's final rejection of the claims of Group E be overturned.

The Nevoux and Holmes References Cannot Support a Proper *Prima Facie* Case of Obviousness for the Claims of Group F

Group F contains claims 6 (dependent from 1), 7 (dependent from 6) and 14 (dependent from 9). Accordingly, those claims are patentable for the same reasons presented above for the claims of Group A. But these claims also contain further limitations not suggested by the prior art. The following analysis uses claim 14 as a representative claim for this Group, as that is the dependent claim that the Examiner addressed explicitly.

Claim 14 recites *a control channel between the access means and the authentication means to send an authentication message between the access means and the authentication means, the authentication message including validating information about the access means, the wireless device, and the operator.* According to the Examiner's final rejection, SAA and HLR disclose the recited access means and the authentication means. Final Office Action, page 5. Nevoux's system, however, does not enable the *authentication* of the SAA, and therefore there cannot be an *authentication message* containing *validating information about the access means.*

In summary, neither of the Examiner's references teach or suggest the limitations of claims 6, 7, and 14, under any reasonable interpretation of those limitations. Thus combining the references, as the Examiner suggests, is to no avail. A *prima facie* case of obviousness is lacking, and the claims of Group F must be allowed. Applicant respectfully requests that the Examiner's final rejection of the claims of Group F be overturned.

The Nevoux and Holmes References Cannot Support a Proper *Prima Facie* Case of Obviousness for the Claims of Group G

Group G contains claims 8 (dependent from 6), 15 (dependent from 13) and 20 (dependent from claim 16). Accordingly, claims 8 and 15 are patentable for the same reasons presented above for the claims of Group A, and claim 20 is patentable for the same reasons presented below for claims of Group H. But these claims also contain further

limitations not suggested by the prior art. The following analysis uses claim 13 as a representative claim for this Group, as that is the dependent claim that the Examiner addressed explicitly.

Claim 15 recites *communications between the wireless device and the access means and over the control channel are encrypted.* According to the Examiner's final rejection, Nevoux's system discloses "two distinct cryptographic functions AG and AT to calculate session keys and to handle the communication [see column 4 lines 8-23]." The AG calculates session keys in SIM and HLR and the AT calculates session keys in PA and VLR. The only signals enabled by Nevoux's system that are transmitted between PA and SAA and over the control channel to HLR are the identification parameters IMUI and IMTI. These identification parameters are, however, not session keys and therefore not encrypted by AG or AT. Thus, communications, in Nevoux's system, between the PA and the SAA and over the control channel to the HLR are not encrypted.

In summary, neither of the Examiner's references teach or suggest the limitations of claims 8, 15, and 20, under any reasonable interpretation of those limitations. Thus combining the references, as the Examiner suggests, is to no avail. A *prima facie* case of obviousness is lacking, and the claims of Group G must be allowed. Applicant respectfully requests that the Examiner's final rejection of the claims of Group G be overturned.

The Nevoux and Holmes References Cannot Support a Proper *Prima Facie* Case of Obviousness for the Claims of Group H

Group H contains claims 16 (independent) and 19 (dependent from 16). Claims 16 and 19 incorporate concepts from Groups A, B, C, D, and F. Accordingly, claims 16 and 19 are patentable for the same reasons presented above for the claims of Groups A, B, D, and F. Claims 16 and 19 also contains further limitations not suggested by or otherwise obvious from the prior art. The following analysis uses claim 16 as a representative claim for this Group, as that is the broadest claim in the Group.

According to the Examiner's final rejection claims 16 and 19 were rejected for the same reasons as claims 2-8, 10-12, and 14-15. Claim 16 recites:

generating a first authentication message including validating information about an access point connected to a wired LAN,

transmitting the first authentication message from the access point to a wireless

device over a wireless channel,

validating the access point by analyzing the first authentication message without going through a firewall mean.

Nevoux's system fails to meet the limitations in claim 16 under similar arguments given in Group B and F. In particular, Nevoux's system cannot disclose a first authentication message including validating information about an access point because Nevoux's system does not authenticate an access point.

Claim 16 further recites:

transmitting the first and second authentication messages to an authentication server after validating the access point and the wireless device without going through the firewall means;

validating the operator, the wireless device, and the access point without going through the firewall means; and

enabling a data channel between the wireless device and other devices on the wired LAN after validating the operator, the wireless device, and the access point,

where validating the access point, the wireless device, and the operator occurs at an authentication means.

Nevoux's system fails to meet the limitations in claim 16 under similar arguments given in Group B, D, and F. In particular, Nevoux's system does not enable the authentication of an access point, nor does it disclose an authentication server.

In summary, neither of the Examiner's references teach or suggest the limitations of claims 16 and 19, under any reasonable interpretation of those limitations. Thus combining the references, as the Examiner suggests, is to no avail. A *prima facie* case of obviousness is lacking, and the claims of Group H must be allowed. Applicant respectfully requests that the Examiner's final rejection of the claims of Group H be overturned.

The Nevoux and Holmes References Cannot Support a Proper *Prima Facie* Case of Obviousness for the Claims of Group I

Group I contains claims 17 (dependent from 16) and 18 (dependent from 17). Accordingly, those claims are patentable for the same reasons presented above for the claims of Group H. But these claims also contain further limitations not suggested by the prior art. Claims 17 and 18 incorporate concepts from Groups B and C. The following

analysis uses claim 17 as a representative claim for this Group, as that is the broadest claim in the Group.

Claim 17 recites *transmitting the first authentication message includes transmitting information about the access point contained in a first authentication device.* Nevoux's system fails to meet the limitations in claim 17 under similar arguments given in Group B and F. In particular, Nevoux's system does not enable the authentication of an access point nor disclose a first authentication device.

In summary, neither of the Examiner's references teach or suggest the limitations of claims 17 an 18, under any reasonable interpretation of those limitations. Thus combining the references, as the Examiner suggests, is to no avail. A *prima facie* case of obviousness is lacking, and the claims of Group I must be allowed. Applicant respectfully requests that the Examiner's final rejection of the claims of Group I be overturned.

APPENDIX

37 CFR §1.192(c) (9)

The text of the claims on appeal is:

1. (Previously presented) A secure wireless local area network (LAN), comprising:

a firewall to control access to a wired computer LAN;

a wireless device coupled to a wireless device operator;

an access point coupled to the wired computer LAN in communication with the wireless device through an air channel to authenticate the wireless device without going through the firewall; and

an authentication server coupled to the wired computer LAN to provide the operator with access to the wired LAN after authenticating the access point, the wireless device, and the operator without going through the firewall.

2. (Previously presented) The secure wireless LAN of claim 1 where the access point includes a first authentication device to send a first authentication message to the wireless device, the second authentication message including validating information about the access point.

3. (Previously presented) The secure wireless LAN of claim 2 where the wireless device includes a second authentication device to send a second authentication message to the access point, the first authentication message including validating information about the wireless device and the operator.

4. (Previously presented) The secure wireless LAN of claim 3 where the access point sends the first and second authentication messages to the authentication server after authenticating the wireless device.

5. (Previously presented) The secure wireless LAN of claim 3 where the first and second authentication devices are smart cards.

6. (Previously presented) The secure wireless LAN of claim 1 including a control channel between the access point and the authentication server to send an authentication message between the access point and the authentication server, the authentication

message including validating information about the access point, wireless device, and operator.

7. (Original) The secure wireless LAN of claim 6 including a data channel on the wired LAN for sending data from the wireless device to any other device coupled to the wired LAN, the data channel being enabled after the authentication message is validated by the authentication server.

8. (Previously presented) The secure wireless LAN of claim 6 where the communications between the wireless device and the access point and over the control channel is encrypted.

9. (Previously presented) A secure wireless local area network (LAN), comprising:

a firewall means to control access to a wired computer LAN;

a wireless means for use by a wireless device operator;

an access means coupled to the wired computer LAN to authenticate the wireless means without going through the firewall means;

an authentication server means coupled to the wired computer LAN to enable the operator's access through the wireless access means to the wired computer LAN after authenticating the access means, the wireless device, and the operator without going through the firewall means.

10. (Previously presented) The secure wireless LAN of claim 9 where the access means includes a first authentication means to generate, encrypt, and transmit a first authentication message to the wireless means, the first authentication message including validating information about the access means.

11. (Previously presented) The secure wireless LAN of claim 10 where the wireless device includes a second authentication means to generate, encrypt, and transmit a second authentication message to the access means, the second authentication message including validating information about the wireless device and the operator.

12. (Previously presented) The secure wireless LAN of claim 11 where the first

authentication means transmits the first and second authentication messages to the authentication means after authenticating the wireless device.

13. (Previously presented) The secure wireless LAN of claim 11 where the first and second authentication means are smart cards.

14. (Previously presented) The secure wireless LAN of claim 9 including a control channel between the access means and the authentication means to send an authentication message between the access means and the authentication means, the authentication message including validating information about the access means, the wireless device, and the operator.

15. (Previously presented) The secure wireless LAN of claim 13 where communications between the wireless device and the access means and over the control channel are encrypted.

16. (Currently amended) A method for operating a local area network (LAN), comprising:

generating a first authentication message including validating information about an access point connected to a wired LAN;

transmitting the first authentication message from the access point to a wireless device over a wireless channel;

validating the access point by analyzing the first authentication message without going through a firewall means;

generating a second authentication message including validating information about the wireless device and a wireless device operator;

transmitting the second authentication message from the wireless device to the access point;

validating the wireless device by analyzing the second authentication without going through the firewall means;

transmitting the first and second authentication messages to an authentication server after validating the access point and the wireless device without going through the firewall means;

validating the operator, the wireless device, and the access point without going through the firewall means; and

enabling a data channel between the wireless device and other devices on the wired LAN after validating the operator, the wireless device, and the access point,

where validating the access point, the wireless device, and the operator occurs at an authentication means.

17. (Previously presented) The method of claim 16 where transmitting the first authentication message includes transmitting information about the access point contained in a first authentication device.

18. (Previously presented) The method of claim 17 where transmitting the second authentication message includes transmitting information about the wireless device and the operator contained in a second authentication device.

19. (Previously presented) The method of claim 16 where transmitting the first and second authentication messages includes establishing a control channel between the access point and the authentication server.

20. (Original) The method of claim 16 including encrypting information transferred over the wireless and control channel.

CONCLUSION

The Appellant requests favorable consideration by the Board. If any questions remain, please call the undersigned.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

Graciela G. Cowger
Reg. No. 42,444

MARGER JOHNSON & McCOLLOM, P.C.
1030 SW Morrison Street
Portland, OR 97205
(503) 222-3613

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
Date: August 9, 2004

Lisbeth A. Nichols